ABSTRACT

A security device is disclosed. In one embodiment, the security device includes a memory device comprising having a first memory portion configured to store a device ID; and a second memory portion configured to store a device secret. The security device further includes a processor connected to the memory device wherein the processor is configured to read the stored device ID from the first memory portion and the stored device secret from the second memory portion and perform a nonreversible computation using the stored device ID, the stored device secret, and a challenge as seeds. Additionally, the security device includes a communication circuit connected to the processor, the communication circuit configured to receive the challenge from a host device and to communicate a result of the nonreversible computation performed by the processor.